

EXHIBIT 12

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X
IN THE MATTER OF AN APPLICATION FOR A
SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS
100 COLIN DRIVE, HOLBROOK, NY 11741
-----X

141

921

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH
WARRANT

EASTERN DISTRICT OF NEW YORK, SS:

MATTHEW CALLAHAN, being duly sworn, deposes and states that he is a
Special Agent with the Federal Bureau of Investigation (FBI), duly appointed according to
law and acting as such.

Upon information and belief, there is probable cause to believe that there is
located in THE PREMISES KNOWN AND DESCRIBED 100 COLIN DRIVE,
HOLBROOK, NY 11741 (the "PREMISES"), further described in Attachment A, the things
described in Attachment B, which constitute evidence, fruits and instrumentalities of mail
fraud, in violation of 18 U.S.C. § 1341; wire fraud, in violation of 18 U.S.C. § 1343; theft of
government funds, in violation of 18 U.S.C. § 641; and conspiracy to launder money, in
violation of 18 U.S.C. § 1956 (h); as well as obstruction of justice, in violation of 18 U.S.C.
§§ 1512(c) and 1519; and making false statements to law enforcement officers, in violation
of 18 U.S.C. § 1001.

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the FBI. I have been employed by the FBI for more than five years. For over three and a half years, I have been assigned to a corporate and securities fraud squad in the FBI's New York Field Office. I am responsible for investigating various types of crimes, including insider trading, market manipulation, ponzi schemes, and accounting fraud. I have participated in the execution of search warrants, including search warrants involving electronic evidence. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. Although the investigation at issue herein has been led by the Philadelphia Field Office of the FBI, in coordination with the Department of Defense Criminal Investigative Service, I have discussed this investigation with the Philadelphia case agent, and I am familiar with the facts set forth below. The information in this Affidavit is based on my training, and information relayed to me by other law enforcement officers from their investigation including interviews, information obtained from cooperating witnesses, surveillance, and review of records, including bank records, documents obtained in the course of the investigation by grand jury subpoenas, records obtained through search

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

warrants, and other government records. I submit this Affidavit for the limited purpose of establishing probable cause for the search warrant; therefore I have not recited every fact know to law enforcement about this investigation.

3. I am also aware that a federal grand jury has returned an indictment in the United States District Court for the Eastern District of Pennsylvania on October 23, 2014, Criminal Case Number 14-CR-574. I am familiar with that indictment, which is currently under seal. That indictment charges that DEVOS LTD, d/b/a GUARANTEED RETURNS, its own and Chief Executive Officer, DEAN VOLKES, have engaged in a mail and wire fraud scheme involving an excess of \$116 million, in violation of 18 U.S.C. §§ 1341 and 1343; and theft of more than \$14 million in government funds, in violation of 18 U.S.C. § 641. It further alleges that they, together with GUARANTEED RETURNS' Chief Financial Officer, DONNA FALLON, who is the sister of CEO Dean Volkes, have engaged in a conspiracy to launder the funds of the fraud, in violation of 18 U.S.C. § 1956(h), and that they conspired with a member of GUARANTEED RETURNS' information technology team, RONALD CARLINO, to obstruct justice and lie to federal investigators, in violation of 18 U.S.C. §§ 371, 1512(c), 1519, and 1001. I have attached a copy of the sealed indictment to this Affidavit as Exhibit A.

I. BACKGROUND

4. GUARANTEED RETURNS is a "reverse distributor" of pharmaceutical products for healthcare provider clients located throughout the United States; its clients include United States government agencies. DEAN VOLKES is the President,

Chief Executive Officer, and owner of GUARANTEED RETURNS, and his sister, Donna Fallon, is the company's Chief Financial Officer. GUARANTEED RETURNS has its main place of business at 100 Colin Drive, Holbrook, NY and operates a separate warehouse in Ronkonkoma, NY.

5. Health care provider clients of GUARANTEED RETURNS, including clients related to the Department of Defense, sent their expired or excess pharmaceutical products to GUARANTEED RETURNS, with the expectation that GUARANTEED RETURNS would submit the pharmaceuticals to the appropriate manufacturers or the manufacturer's wholesaler for refund. GUARANTEED RETURNS inventoried those products and coordinated the return of those products to the manufacturer of each product or to the wholesaler as the manufacturer's agent. Pharmaceutical wholesalers issued the refunds to GUARANTEED RETURNS, which was expected to deliver the funds, less a fee for its service, to its healthcare provider clients via check or credit back to the client's wholesaler account.

6. Since at least 1999, GUARANTEED RETURNS has increased its profits by stealing certain of its healthcare provider clients' drug product returns, thereby defrauding its clients of millions of dollars each year.

A. Initiation of the Investigation

7. This investigation began as a result of funds missing from the return of certain drugs by the District of Columbia Department of Health through GUARANTEED RETURNS, under a sole source contract between GUARANTEED RETURNS and the

Department of Defense (“DoD”). Under this contract, GUARANTEED RETURNS was the exclusive provider of pharmaceutical returns services for DoD and certain other federal government entities between 2001 and 2007. The investigation determined that the GUARANTEED RETURNS employee responsible for the DoD contract, the Vice President of National Accounts and Government Affairs (“Vice President/National Accounts”), stole more than one-million dollars from the DoD, by causing checks properly issued to DoD entities to be cancelled and re-issued to a shell company controlled by the Vice President/National Accounts and his confederates.²

B. Destruction of Records/Obstruction of Justice

8. On or about September 14, 2009, DCIS agents served DEAN VOLKES with a federal grand jury subpoena requiring GUARANTEED RETURNS to produce records related to the DoD contract (“the grand jury subpoena”). GUARANTEED RETURNS quickly embarked on a record destruction campaign, deliberately destroying years’ worth of computer files that were responsive to the grand jury subpoena, in order to conceal its own diversion of pharmaceutical product and refunds. See Indictment, Count 35.

C. The FilePro Computerized Inventory System Provided Evidence that Numerous “Indate” Products Were Stolen From Clients

9. Investigation showed that GUARANTEED RETURNS and its senior management destroyed records responsive to the grand jury subpoena because GUARANTEED RETURNS had for years been involved in a fraudulent scheme to steal

²The GUARANTEED RETURNS Vice President/National Accounts was charged by indictment with violations of 18 U.S.C. §§ 641, 1031, 1341, and 1343. He pleaded guilty to the indictment on February 17, 2011.

“indate” return product from its clients and retain the corresponding manufacturers’ refunds for itself.

10. GUARANTEED RETURNS manages the returns of pharmaceutical products for healthcare provider clients. GUARANTEED RETURNS’ marketing materials emphasize the company’s expertise in tracking and returning pharmaceutical products, and reconciling its clients’ return credits, emphasizing visibility and “100% accountability and inventory management systems.” GUARANTEED RETURNS charges its clients a fee for, among other services, the tracking of returned pharmaceutical products and the manufacturers’ credits due and owing to the clients for the returned product. GUARANTEED RETURNS’ marketing materials promise that GUARANTEED RETURNS will handle the tracking of pharmaceutical products returns and related credits for its clients.³ As described below, DEAN VOLKES and GUARANTEED RETURNS defrauded certain clients by taking advantage of those clients who relied upon GUARANTEED RETURNS’ representations that the company would fairly and honestly track client returns and refunds. In effect, DEAN drew his fraud victims into his scheme by encouraging the victims to rely upon GUARANTEED RETURNS’ tracking and accounting services, and then taking advantage of that reliance by stealing their pharmaceutical products, returning them to the manufacturers for refunds, and keeping the refunds for his company and himself.

³ In fact, GUARANTEED RETURNS’ marketing materials actively discourage independent tracking of products and credits by its clients. The GUARANTEED RETURNS website Frequently Asked Questions (FAQs) page lists the following question and answer: Question: Should I waste my time and effort sorting out certain manufacturers, researching their policies, and track various credits from multiple sources? Answer: NO. Guaranteed Returns performs these activities for you.

11. “Indate” product is product that a healthcare provider client sends to GUARANTEED RETURNS for return to the manufacturer, but which is not yet ripe for return under the manufacturer’s return policy. For example, a manufacturer may be willing to provide a refund on pharmaceutical products for a nine-month window, accepting products that will expire within the next three months or that have been expired for no more than six months. If a client sends product to GUARANTEED RETURNS that will be expiring in four months, that product is “indate” and cannot yet be returned for credit. According to numerous former employees and sales representatives of GUARANTEED RETURNS, clients were told that GUARANTEED RETURNS would accept “indate” product, retain it until it was ripe for return under the manufacturer’s policy, and then return it for the client’s credit. GUARANTEED RETURNS did sort “indate” product. However, GUARANTEED RETURNS routinely converted the “indate” product to its own use, then kept the resulting refund for itself rather than remitting the return funds to the client.

12. The diversion of the “indates” from the clients to GUARANTEED RETURNS was accomplished via GUARANTEED RETURNS’ computerized inventory system, using a program known as FilePro. The computer programmer who wrote the code to accomplish this theft, identified in the Indictment as Person #1, asserts that he did this at the specific direction of DEAN VOLKES. He states that VOLKES personally determined which clients would receive the funds for their “indate” product and which clients would not. VOLKES had a list, called the “managed table,” of clients who were permitted to receive their “indates.” Any client not on the “managed table” did not receive refunds for “indate”

products. Instead, the FilePro system would designate the products to a “GRX” or GUARANTEED RETURNS account, a so-called “GRX store,” at the time the products were to be returned to the manufacturer. When the manufacturer sent GUARANTEED RETURNS a check or electronic transfer of funds for these products, GUARANTEED RETURNS would simply retain the funds for itself, and would not pay the refund for the indated product to its client. See Indictment, Count One, ¶¶ 29-34.

13. In addition to using the FilePro system to divert indate products into GUARANTEED RETURNS’ own account, DEAN VOLKES directed Person #1 to program additional diversion strategies into the FilePro inventory system. In January 2011, VOLKES directed Person #1 to examine indated products to determine when they had been received by GUARANTEED RETURNS. All products that had been received more than three years before they were ultimately eligible for return were to be diverted to a so-called GRX Store. Additionally, VOLKES directed Person #1 to implement a “G-13” program, in which every thirteenth product for “managed” clients was reviewed to determine whether it could be treated as “unmanaged.” Products that were worth more than \$3,000 or for which the refunds would be paid directly to the client (rather than to GUARANTEED RETURNS) were excluded. However, if a product was not excluded by one of the G-13 Program rules, it was diverted from the “managed” customer to a so-called GRX Store. See Indictment, Count One, ¶¶ 35-39.

14. According to Person #1, as well as other former employees and sales representatives of GUARANTEED RETURNS, clients would occasionally contact their

sales representative to inquire about the status of “indate” product. If a client specifically inquired, GUARANTEED RETURNS would then issue a check to the client for the value of the product. However, if the client did not inquire, the funds remained with GUARANTEED RETURNS.

D. The FilePro Computerized Inventory System Provided Evidence of the Fraud Proceeds

15. On March 29, 2011, the Honorable Marilyn Go, United States Magistrate Judge for the Eastern District of New York, approved applications for five warrants to search locations related to GUARANTEED RETURNS’ obstruction and diversion schemes, including the business locations of GUARANTEED RETURNS and certain employee residences. On April 5, 2011, agents executed the warrants and seized voluminous documents, electronic evidence, records and other items related to the investigation.

16. Among the records obtained pursuant to the warranted search on the GUARANTEED RETURNS business premises was the FilePro server.⁴ The FilePro server hosts the inventory records, as well as the computer code that was used to divert the

⁴ The FilePro Server was seized during the April 5, 2011 search, imaged, and returned. Law enforcement agents who specialize in recovery of evidence from computers, who were involved in the imaging of this server, state that the server was identified at that time as NYDATA2. However, they further explain that data servers are, in the normal course of business, replaced, expanded, or otherwise modified, in order to maintain or improve their functionality. Accordingly, while the agents know the name of the server at the date of the search three years ago, that name, or the serial number of the equipment, may have changed in the ensuing time period. Moreover, while Person #1 stated in approximately April 2014 that the FilePro programming code continued to operate to divert unmanaged indates to the GRX Stores, and therefore, the FilePro system will contain evidence of new fraud subsequent to the April 5, 2011 search, servers can be updated at any time, without notice, and therefore, agents cannot inquire about the current name and serial number of the FilePro server without revealing the pendency of a new search.

“indates” from GUARANTEED RETURNS clients to the so-called GRX Stores. Person #1 has assisted investigators in accessing data obtained from the GUARANTEED RETURNS servers as a result of the search warrant, as well as from the back-up hard drives provided by Person #1.

17. Person #1 assisted federal agents in locating a table within the GUARANTEED RETURNS FilePro system that identified so-called the GRX Stores. The table showed that the following accounts in the FilePro system are all GRX Stores:

<u>GRX Store</u>	<u>Wholesaler</u>
44158-242	Amerisource
22367-15426	Cardinal
22431-753	Amerisource
21322-23410	Amerisource
43703-120	Amerisource
44130-304	Amerisource
45778-530	Amerisource

18. With the assistance of Person #1, investigators were able to download indate data including the period of 2007 to on or around April 5, 2011, the date the search warrants were executed. This indate data was generated from the GUARANTEED RETURNS FilePro inventory system seized during the execution of search warrants and from two hard drives provided by Person #1, containing data backed up by Person #1 in or around 2009, which Person #1 maintained in his residence. This indate data details all indates processed by GUARANTEED RETURNS during that time period. One field within the data details the original store (that is, client) to which the drug product was assigned. Another field details the store to which the product was assigned at the time it was returned

to the wholesaler. In some cases, the fields are identical, and the clients who provided the indate product are properly designated to receive the refunds due and owing to those clients for the returned product. In other cases, the second field, "the re-processing field," has changed, and the product has been designated to a so-called GRX Store.

19. Using the "re-processing field," investigators were able to extract from the indate data all transactions that were identified as having been re-processed through the GRX Stores above, and identify their corresponding batches. Through an examination of the batch details, investigators were able to identify the store (that is, client) to which the product had originally been assigned and the corresponding product details. Since GUARANTEED RETURNS gives an "estimated return value" to the product it reprocesses for return to manufacturers and diverts from its clients, investigators were able to calculate the estimated return value for the product re-processed through each of the so-called GRX Stores and quantify the approximate value of the drug products stolen from the original clients by DEAN VOLKES and GUARANTEED RETURNS.

20. Using an additional database within the GUARANTEED RETURNS FilePro system, known as the Store Summary file, investigators were able to confirm the dollar amount of DEAN VOLKES' and GUARANTEED RETURNS' fraud. The Store Summary file is a database which contains a summary of data for each client account (referred to as a "store" by the software), including the value of product attributable to each store, and tracks, among other things, refund distributions or payments attributable to batches

and stores. Utilizing the Store Summary file, investigators were able to calculate the amount of product diverted from GUARANTEED RETURNS clients.

21. Through an examination of information stored on the servers and hard drives related to DEAN VOLKES' indate managed FilePro table, other electronically stored information regarding indate returns and related refunds, records obtained from wholesalers, and from information provided by Person #1 and other witnesses, investigators have determined that up to the date of the execution of the search warrants, VOLKES diverted product in the amount of at least approximately \$116,193,369 from GUARANTEED RETURNS' clients to the following so-called GRX stores, in the following corresponding amounts:

<u>GRX Store</u>	<u>Amount</u>	<u>Wholesaler</u>
44158-242	\$62,660,916	Amerisource
22367-15426	\$10,596,608	Cardinal
22431-753	\$41,798,476	Amerisource
21322-23410	\$1,015,603	Amerisource
43703-120	\$42,088	Amerisource
44130-304	\$11,402	Amerisource
45778-530	\$68,276	Amerisource
	<u>\$116,193,369⁵</u>	

E. The Time Inherent in Processing Refunds Means That Evidence Related to Stolen Drugs Continues to Be Created Months After the Theft

22. Data accumulated in the FilePro inventory system since the time of the April 5, 2011 search will provide evidence of the amount of fraud proceeds that DEAN

⁵ The above figures represent only the amount of diverted product as of April 5, 2011, the date that search warrants were executed, when the FilePro server was imaged. Determination of the current value of diverted product will require obtaining the current FilePro data.

VOLKES and GUARANTEED RETURNS obtained for drug products that were stolen, i.e., diverted to a so-called “GRX Store,” prior to the search because of the delays inherent in the returns process.

23. GUARANTEED RETURNS uses a “batch” process to return its clients’ pharmaceutical products to manufacturers. In its batch process, GUARANTEED RETURNS consolidates several hundred products from several hundred different clients into a batch associated with a particular wholesaler. GUARANTEED RETURNS then sends returns from that batch to numerous manufacturers, and requests that credit or a check be issued to the wholesaler. Stolen indates are returned to manufacturers in “batches” together with products that are being returned for legitimate clients. As a result, when the manufacturer issues a refund to a wholesaler for a batch of returns, the fraud proceeds for the diverted indates are commingled with legitimate client funds.

24. Wholesalers attribute payments to specific GUARANTEED RETURNS batches. GUARANTEED RETURNS then allocates the payment received for that batch across the clients that had products in the batch, including the so-called “GRX Stores.” When this attribution is made, it is applied in the FilePro system to show that a refund was received.

25. By way of example, using data obtained from the search warrants at GUARANTEED RETURNS as well as other data obtained from Person #1 and subpoenaed records, investigators has analyzed refund payment distributions by GUARANTEED RETURNS for batches processed through store 44158-242 (Amerisource). Batch #35 dated

March 16, 2011, shortly before the date of the execution of the search warrants, appears, based on these records, have been sent to manufacturers for refund on or around March 31, 2011. GUARANTEED RETURNS started receiving payment from Amerisource for batch #35 in or around May 5, 2011. The “estimated return value” in FilePro for this batch was \$4.9 million. This amount includes fraud proceeds of approximately \$2.2 million. Because payments had not been received for this batch by the date of the April 5, 2011 search, investigators do not have the GUARANTEED RETURNS records related to return payment allocations for batch #35. These records, as well as allocation records related to other batches for which funds were received from wholesalers after the date of the search warrants, remain in the possession of GUARANTEED RETURNS.

F. Evidence That Will Be Found in the SUBJECT COMPUTER SYSTEM

26. Records contained in the FilePro inventory management system, within the SUBJECT COMPUTER SYSTEM, will contain evidence of the additional amount of fraud proceeds received by GUARANTEED RETURNS after the date of the search warrant. As set forth above, this includes the “managed list,” the table of “GRX Stores,” the “managed table” and the computer code that stole products based on that table, the G-13 computer code, the “re-processing field,” and the Store Summary files.

27. In addition to those fraud proceeds from the product already re-processed for payment at the time of the execution of the search warrants, investigators believes that DEAN VOLKES and GUARANTEED RETURNS have continued the fraud scheme related to “indate” product. Person #1 has testified that DEAN VOLKES directed

him to disable the “G13” program shortly after the execution of the search warrants on April 5, 2011. However, VOLKES did not direct Person #1 to disable the “managed table” and related computer code or the “3- Year Cutoff” program. Moreover, VOLKES did not direct Person #1 to change the indate records for product that was re-processed to the “GRX Stores” back to the original clients. Accordingly, there is probable cause to believe that this aspect of the fraud scheme is still in operation.

II. THE PREMISES

28. The PREMISES at issue here, as further described in Attachment A, are the business premises of defendant GUARANTEED RETURNS, located at 100 Colin Drive, Holbrook, NY 11741. This Affidavit seeks the limited authority to search these PREMISES, in order to seize evidence from the computer servers that contain the GUARANTEED RETURNS FilePro inventory system, including all data, tables and records upon which the FilePro system relies (the SUBJECT COMPUTER SYSTEM).

29. I have been informed by an Assistant U.S. Attorney that, under the relevant case law, in the event of a search of business premises that are “permeated with fraud,” a broad search warrant that authorizes the search and seizure of voluminous business records does not run afoul of the Fourth Amendment. National City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980) (citing United States v. Brien, 617 F.2d 299, 309 (1st Cir. 1980)); see also United States v. Johnson, 108 F.3d 1370, 1997 WL 136332, at *3 (2d Cir. Mar. 21, 1997) (unpublished summary order) (affirming broad search where affidavit “show[ed] ample ground for finding pervasive fraud”). As demonstrated by the

facts set forth above, as well as the Indictment, defendant GUARANTEED RETURNS is a business permeated by fraud. The fraud and money laundering scheme set forth in the Indictment has been underway since at least 1999. They have engaged in numerous different strategies to engage in the fraud, surreptitiously stealing all indated product from some customers, the thirteenth indated product from other customers, and product that has been sitting for more than three years from all customers. *See* Indictment Count One, at ¶¶ 28-38. Moreover, when clients inquire about missing product, GUARANTEED RETURNS refunds the amount stolen in order to conceal the scheme. When investigators sought information about another crime, that might have alerted investigators to the indate scheme, employees of GUARANTEED RETURNS lied to investigators and destroyed the relevant records, in defiance of a grand jury subpoena. Given these facts, a search of the PREMISES in order to obtain the seizure of the SUBJECT COMPUTER SYSTEM is warranted.

IV. TECHNICAL BACKGROUND

30. As described above and in Attachment B, this application seeks permission to search for records constituting evidence, fruits or instrumentalities of violations of mail fraud, wire fraud, theft of government funds, obstruction of justice and lying to federal agents that might be found on the PREMISES, in the SUBJECT COMPUTER SYSTEM. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if the SUBJECT COMPUTER SYSTEM, including components such as a computer⁶ or storage medium,⁷ is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In

⁶ For purposes of the requested warrant, a computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

⁷ A “storage medium” for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs and DVDs, and flash drives.

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of evidence related to this investigation and witness statements in this case, as noted in the Indictment, Count 1, paragraphs 29 to 39, and Count Thirty-Five, paragraphs 16 to 18, computer equipment was used in this case in furtherance of the scheme to defraud the government and others through wire and mail fraud, as well as the scheme to obstruct justice by destroying computer records. Agents in this case have been informed by Person #1 that the SUBJECT COMPUTER SYSTEM still exists and is inactive use. There is reason to believe that there is a computer system currently located on the PREMISES.

32. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic “attribution” evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, Internet search histories,

configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. In lieu of removing storage media from

the premises, it is sometimes possible to “image” the data stored on such devices. Generally speaking, imaging is the taking of a complete electronic picture of the computer’s data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the time required for examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the

storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would authorize seizing, imaging, or otherwise copying computers and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. I recognize that DEVOS LTD d/b/a GUARANTEED RETURNS (“GUARANTEED RETURNS”) is a functioning company with many employees, and that a seizure of GUARANTEED RETURNS’ computers may have the unintended effect of limiting GUARANTEED RETURNS’ ability to conduct its legitimate business. As with any search warrant, I expect that officers executing this warrant will take appropriate steps to execute the warrant reasonably and avoid causing unnecessary inconvenience to GUARANTEED RETURNS, its employees, and its customers. Such steps may include:

a. Identifying a system administrator of the network (or other knowledgeable employee) who would be willing to assist law enforcement by identifying,

locating, and copying the things described in the warrant; imaging items on-site, as described above; and,

b. If imaging proves impractical, or even impossible for technical reasons, seizing those components of GUARANTEED RETURNS' computer system that are necessary to conduct an off-site examination. The seized components would be removed from the PREMISES. If employees of GUARANTEED RETURNS so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of GUARANTEED RETURNS' legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

VI. CONCLUSION

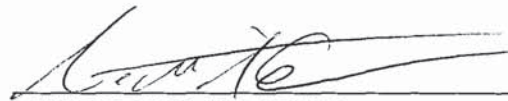
36. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the PREMISES there exists evidence of crimes. Accordingly, a search warrant is requested.

37. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary. This affidavit refers to an indictment that is currently under seal in another judicial district. Moreover, the defendants in this case have aggressively obstructed justice in the past by deleting data from their computer systems. Premature disclosure of the contents of this

affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS **100 COLIN DRIVE, HOLBROOK, NEW YORK 11741.**

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.



MATTHEW CALLAHAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
4th day of October, 2014



THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A
Property to Be Searched

100 Colin Drive, Holbrook, New York 11741

The business office and warehouse located at 100 Colin Drive, Holbrook, NY 11741 is further described as a one-story cement block building located on the corner of Colin Drive and Andrea Road. There is a sign containing the language "Guaranteed Returns" and the number "100" located on the north end of the building. The main entrance consists of double glass doors located on the northeast corner of the building containing the language "Guaranteed Returns." There is a grey door located on the southeast corner of the warehouse facing east, containing in black letters "GUARANTEED RETURNS." On the southeast corner of the building facing south is a warehouse bay door containing black letters "GUARANTEED RETURNS GROUND LEVEL RECEIVING." Also on the south side of the building are three additional white warehouse bay doors two of which contain in black letters "GUARANTEED RETURNS SHIPPING and the eastern-most door containing in black letters "GUARANTEED RETURNS."

SW000114

ATTACHMENT B

Items to Be Seized

The items which constitute evidence, fruits and instrumentalities of mail fraud, in violation of 18 U.S.C. § 1341; wire fraud, in violation of 18 U.S.C. § 1343; theft of government funds, in violation of 18 U.S.C. § 641; and conspiracy to launder money, in violation of 18 U.S.C. § 1956 (h); as well as obstruction of justice, in violation of 18 U.S.C. §§ 1512(c) and 1519; and making false statements to law enforcement officers, in violation of 18 U.S.C. § 1001, are further described as follows:

Computers, servers and computer-related equipment containing all records of the FilePro computerized inventory system, including all data, tables and records, upon which the FilePro system exists. *relies on*